RAPORT CERT NASK - 1997 rok

W 1997 roku CERT NASK kontynuował swoją programową działalnoć nakreśloną na początku 1996 roku. Jej głównym zadaniem była obsługa zdarzeń naruszających bezpieczeństwo sieci. Wraz z rozwojem internetu wzrasta ilość przypadków wykraczających poza ramy ogólnie przyjętej etykiety sieciowej. CERT NASK, podobnie jak większoć tego typu zespołów odnotowały wyraźny wzrost incydentów naruszających bezpieczeństwo. Wiele z tych przypadków zgłaszanych jest do CERT NASK.

W 1997 roku CERT NASK przyjął kilkadziesiąt zgłoszeń dotyczących zdarzeń, które naruszały zasady netykiety, wiele z nich naruszało także bezpieczeństwo sieci. Większość ze zgłoszonych incydentów w sposób poważny naruszało bezpieczeństwo sieci Internet, zarówno polskiej jej części jak i sieci Internet w ogóle. W ciągu omawianego okresu nie zauważyliśmy wyraźnych zmian w sposobach ataków sieciowych. Niepokojącym może się jedynie okazać zjawisko wzrostu wykorzystania narzędzi atakujących poprzez niedoświadczonych, posiadających niski poziom wiedzy technicznej, intruzów.

Wśród dominujących typów ataków sieciowych znalazły się następujące:

- ataki na słabe hasła użytkowników
- ataki na serwery informacyjne, tzw. news servers
- ataki na programy obsługujące pocztę elektroniczną
- ataki typu mail bombing, rozpowszechnianie przez sieć szkalujących informacji, naruszających dobra osobiste poszkodowanego

Inne, rzadsze rodzaje ataków to:

- próby odnalezienia słabych stron systemów komputerowych za pomocą programów skanujących
- ataki mające na celu naruszenie treści stron WWW
- ataki na serwer IMAP (Internet Message Access Protocol)
- ataki poprzez programy typu CGI (Common Gateway Interface)

Ataki na serwery informacyjne są typowym przykładem zjawiska wykorzystywania narzędzi sieciowych służących do wykorzystywania słabości oprogramowania działającego w sieci Internet. Specyfika tego typu zagrożenia polega na tym, że w wyniku jednej próby ataku zostaje jednocześnie zaatakowanych wiele serwerów, często zarówno w kraju jak i za granicą. Narzędzia do tego typu ataków często umiejscawiane są w sieci Internet na stronach prywatnych osób, które "reklamują" się jako hackerzy. W przypadku odnalezienia tego typu stron CERT NASK interweniował u właścicieli serwerów, na których tego typu strony się znajdowały. W wyniku takich interwencji strony te były usuwane z serwerów. Wśród incydentów związanych z pocztą elektroniczną bardzo niepokojący jest wzrost zjawiska spammingu. Programy obsługujące pocztę elektroniczną są także przedmiotem ataków w celu uzyskania nieuprawnionego dostępu do serwerów . Głównie były to ataki na program sendmail.

Spamming to wysyłanie przesyłek o treściach najczęściej reklamowych do dużej liczby odbiorców w Internecie. Są to przesyłki nie zamówione i niechciane przez odbiorców zaśmiecające skrzynki pocztowe. Obrona przed spammingiem poprzez odpowiednie konfigurowanie programów pocztowych i instalowanie dodatkowego oprogramowania filtrującego jest istotnym składnikiem bezpiecznego systemu pocztowego.

Aktualizacja i "łatanie" programu sendmail w większości przypadków jest z kolei skuteczną obroną przed atakami typu włamania, gdyż ataki tego typu są również często przeprowadzane przez osoby posiadające niski poziom wiedzy technicznej.

Mail bombing dla odmiany to atak polegający na przesyłaniu do konkretnego użytkownika sieci lub grupy użytkowników dużej ilości listów, często o dużych rozmiarach, które skutecznie paraliżują pracę posiadaczy kont internetowych. Obsługa tego typu zdarzeń nie jest zadaniem łatwym. Z doświadczenia zespołu CERT NASK wynika, że skuteczne ograniczenie tego typu działalności wymaga dużego wysiłku i konsekwencji. Współpraca z dostarczycielami usług internetowych, mimo ich zaangażowania i dobrej woli, często daje niewielkie efekty. Osoba naruszająca netykietę z łatwością może zmienić swojego usługodawcę. Dodatkowym problemem - ułatwiającym intruzom tego typu działalność jest rozpowszechniona, zarówno za granicą jak i w Polsce, możliwość zakładania darmowych kont internetowych, oraz korzystanie z sieci Internet w sposób anonimowy.

Sieć Internet jest także wykorzystywana jako medium do rozpowszechniania szkalujących informacji, naruszających dobra osobiste poszkodowanego. Taki typ ataku dotyczył szczególnie firm komercyjnych. Internet, jako obszar wolny od cenzury, jest doskonałym miejscem do dowolnego

atakowania słownego osób fizycznych lub prawnych. CERT NASK zajmuje się tylko i wyłącznie technicznymi aspektami tych przypadków, nie interpretuje zaś i nie zajmuje stanowiska wobec wyrażonych poprzez Internet opinii, oczywiście jeżeli nie naruszają one prawa. Jeżeli w wyniku działalności poprzez Internet zostaje naruszone dobre imię jednego z jej użytkowników, to ewentualna decyzja o wkroczeniu na drogę prawną należy do poszkodowanego.

W wyniku ataków zgłoszonych do CERT NASK, w około 30% przypadków odnotowaliśmy ingerencję intruza w system. Niestety 30% tych ingerencji kończy się przejęciem praw administratora zaatakowanego systemu. W tego typu przypadkach nasz zespół szczególnie zwracał uwagę na aspekt dokładnego ustalenia sposobu ataku. Niestety nadal w wielu przypadkach niemożliwością pozostają takie ustalenia, a często końcowe ustalenia nie niosą ze sobą stuprocentowej pewności. Główną przyczyną takiego stanu rzeczy jest niekompletność dostarczonych danych źródłowych od poszkodowanego. Ten fakt związany jest z niszczeniem tego typu danych przez intruza, który "zaciera" za sobą ślady. W takich sytuacjach CERT NASK sugeruję poszkodowanemu instalację oprogramowania, oraz innych mechanizmów podwyższających bezpieczeństwo systemu, który w skuteczny sposób chroni przed całkowitą utratą danych.

W około 40% przypadków, w momencie zgłoszenia incydentu poszkodowany stwierdza brak szkód w wyniku ataku. Niestety jest wysoce prawdopodobne iż, niezauważenie szkód powiązane jest z nieumiejętnością ich zidentyfikowania w pierwszym momencie. W takich przypadkach zespół CERT NASK dostarcza narzędzi, które skutecznie "odnajdują" wiele szkód, często sugerujemy także reinstalację systemu, która to jest najpewniejszym rozwiązaniem.

Optymistycznym zjawiskiem, zaobserwowanym przez nasz zespół, jest coraz częściej występujące rozwiązywanie spraw przez samego poszkodowanego. W tego typu sytuacjach, po konsultacji z poszkodowanym, CERT NASK tylko asystuje w sprawie i jest informowany przez obie strony o postępach w rozwiązywaniu sprawy. CERT NASK przystępuje do aktywnej działalności, tylko na wyraźną prośbę poszkodowanego.

Rozkład czasowy zgłoszeń wskazuje zdecydowanie na pierwszy kwartał 1997 roku. Jest to niewątpliwie związane spadkiem "aktywności" w sieci w okresie letnim i dużą ilością zgłoszeń na początku roku po okresie świątecznym. Niestety spadek aktywności w czasie wakacji jest ściśle powiązany ze wzrostem trudności w kontaktach z administratorami maszyn znajdujących się w sieciach wyższych uczelni.

W ramach działalności programowej CERT NASK w omawianym okresie wzbogacił udostępniane zasoby strony WWW, głównie o narzędzia internetowe. W przypadku natężenia szczególnie niebezpiecznych ataków zespół opracowywał plan ochrony przed nimi. O tego typu zagrożeniach, i sposobach obrony, informowane były osoby odpowiedzialne za bezpieczeństwo poszczególnych sieci lokalnych, na terenie całego kraju.

Około 60% odnotowanych przypadków powiązanych było z atakami na maszyny zagraniczne, a także z atakami z maszyn położonych za granicą. W tego typu przypadkach CERT NASK aktywnie współpracował z innymi, zagranicznymi zespołami reagującymi na przypadki naruszenia bezpieczeństwa sieci. Wśród tych kontaktów, szczególnie intensywne były z CERT'ami z Niemiec i Wielkiej Brytanii.

W omawianym okresie CERT NASK, obsługując zgłoszone incydenty, a także prowadząc programową działalność wymienił, za pomocą poczty elektronicznej, kilkaset, udokumentowanych listów.

Typologia ataków obsłużonych przez CERT NASK - 1997 r.